Patrick Carey (CA Bar No. 308623)
LEXINGTON LAW GROUP, LLP
503 Divisadero St.
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
pcarey@lexlawgroup.com

Attorneys for Plaintiffs and the Putative Class

[Additional Counsel on Signature Page.]

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

NICHOLAS HISSERICH AND A.H., BY AND THROUGH HER GUARDIAN, NICHOLAS HISSERICH, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiffs, v. POWERSCHOOL GROUP LLC and POWERSCHOOL HOLDINGS, INC., Defendants.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Nicholas Hisserich and A.H. by and through her guardian, Nicholas Hisserich (collectively "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against PowerSchool Group LLC and PowerSchool Holdings, Inc. (together, "PowerSchool" or "Defendants") individually and on behalf of all others similarly situated. The following allegations are based upon personal knowledge as to Plaintiffs' own facts, upon investigation by Plaintiffs' counsel, and upon information and belief where facts are solely in the possession of Defendants.

NATURE OF THE CASE

1. Plaintiffs brings this action to remedy the harms by Defendants' failures to adequately and reasonably protect its computer systems and networks, resulting in one of the largest cyberattacks that have impacted K-12 school districts throughout the United States. This preventable cyberattack purportedly discovered by Defendants on December 28, 2024, by which cybercriminals infiltrated Defendants' network, accessed and stole sensitive, personally identifiable information ("PII")[1] of Plaintiffs and the class, from Defendants (the "Data Breach").

2. Plaintiffs' and Class Members' sensitive PII – which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure – was targeted, compromised and unlawfully accessed due to the Data Breach.

3. Defendants acquired, collected, and stored Plaintiffs' and Class Members' PII. Therefore, at all relevant times, Defendants knew or should have known that Plaintiffs and Class Members would use Defendants' services, and for which Defendants would store and/or share sensitive data, including highly confidential PII on their computer systems and networks.

[1] PII generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. §200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, *etc.*).

4. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure the Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized third party – an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Plaintiffs and Class Members in the future.

5. Plaintiffs' and Class Members' have been harmed and their identities are now at risk because of Defendants' negligent conduct because the PII that Defendants collected and maintained has been accessed and acquired by data thieves.

6. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

7. Defendants were responsible for providing inadequate data security measures to protect the sensitive PII that was transmitted using its systems. Defendants knew that the type of personal and sensitive data that it received and transmitted is highly targeted and sought after by hackers who seek to exploit that data for nefarious purposes. Defendants' actions resulting in the Data Breach allowed cybercriminals to cause significant harm to Plaintiffs and Class Members.

8. The Data Breach was a direct and proximate result of Defendants' failure to implement and follow basic security procedures. Plaintiffs and Class Members are students and employees of the school districts whose information was compromised because of the Data Breach.

9. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

10. Plaintiffs bring this Complaint on behalf of themselves and all others who were harmed by the Data Breach. Plaintiffs assert claims for (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) invasion of privacy; (5) unjust enrichment; (6) breach of fiduciary duty; and (7) declaratory and judgment.

11. Plaintiffs bring this class action lawsuit on behalf themselves and all those similarly situated to address Defendants' inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

12. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

13. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

14. Plaintiff Nicholas Hisserich is the father and legal guardian of Plaintiff A.H. At all relevant times, he has been a resident of O'Fallon, Missouri. His daughter attends a school in the City of St. Charles School District in St. Charles, Missouri that uses PowerSchool products. As a result, parent and student PII is submitted through PowerSchool.

15. Plaintiff A.H., a minor, is, and at all relevant times herein, a resident of O'Fallon, Missouri. Plaintiff A.H. brings this suit by and through her father and legal guardian, Nicholas Hisserich, who is, and at all relevant times was, an individual and resident of O'Fallon, Missouri.

16. Defendant PowerSchool Group LLC is a limited liability company with its principal place of business located in Folsom, California, and is owned by Defendants PowerSchool Holdings, Inc.

17. Defendant PowerSchool Holdings, Inc. is a corporation with its principal place of business located in Folsom, California.

18. Defendants received highly sensitive PII from Plaintiffs in connection with the services Defendants provided to Plaintiffs. As a result, Plaintiffs' PII was among the data accessed by an unauthorized third party in the Data Breach.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2) because: (1) there are at least 100 putative Class Members, (2) the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000, and (3) there is minimal diversity because at least one Plaintiff and Defendant are citizens of different states.

20. This Court has specific personal jurisdiction over Defendants because it is a citizen of this District, registered to conduct business in this District, maintains its principle place of business in this District, has continuous and systematic contacts with this District, does substantial business in and within this District, receives substantial revenues from marketing, distribution, and sales in this District, so as to subject itself to the personal jurisdiction of this District, and thus rendering the exercise of jurisdiction by this Court proper and necessary.

21. This Court is the proper venue for this case pursuant to 28 U.S.C. §1391 because a substantial part of the events giving rise to Plaintiffs' claims occurred in California and because Defendants conduct a substantial part of its business within this District.

FACTUAL ALLEGATIONS

Defendants Provide Software and Cloud-based Services for School Operations

22. Defendants together provide innovative K-12 software and cloud-based software to school districts.

23. Defendants are the largest provider of cloud-based education software for K-12 education in the United States, serving more than 75% of students in North America.[2]

24. Defendants' software is used by over 18,000 customers to support more than 60 million students in the United States.[3]

25. Defendants offer a full range of services to help school districts operate, including platforms for enrollment, communication, attendance, staff management, learning systems, analytics, and finance.

26. Due to the nature of its business, Defendants receive and maintain PII for millions of students, parents, and school faculty across the country, including the PII of Plaintiffs and Class Members.

27. Under state and federal law, Defendants had a duty to protect the PII of current and former students and school faculty members, including under Section 5 of the Federal Trade Commission Act ("FTC Act"). It likewise had a duty to promptly alert the students, parents, and school faculty that their PII was accessed by an unauthorized third party and which PII was at issue.

28. Plaintiffs and Class Members are current and former students, parents of students, or employees at of the various school district affected by the Data Breach.

29. In the course of their relationship, students and employees, including Plaintiffs and Class Members, provided Defendants with their sensitive PII.

30. Upon information and belief, in the course of collecting PII from students and employees, including Plaintiffs, Defendants promised to provide confidentiality and adequate security for the data it collected from them through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

---

[2] Carly Page, *Edtech giant PowerSchool says hackers accessed personal data of students and teachers*, TECHCRUNCH (Jan. 8, 2025), https://techcrunch.com/2025/01/08/edtech-giant-powerschool-says-hackers-accessed-personal-data-of-students-and-teachers/#:~:text=The%20California%2Dbased%20PowerSchool%2C%20which,according%20to%20the%20company's%20website.

[3] *Id.*

31. Indeed, Defendants provide on its website that:

> We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure the confidentiality, integrity, and availability of our customers' personal data by leveraging technical, organizational, and where appropriate, physical security methods. Security protection at PowerSchool is a cross-functional activity that intersects our workforce duties, and we have relevant security and privacy policies to drive expectations from the workforce.[4]

32. Plaintiffs and the Class Members, as students or employees at the school districts, relied on these promises and on these sophisticated business entities to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their sensitive PII is involved.

The Data Breach

33. On or about December 28, 2024, PowerSchool, an education technology platform for K-12 education housing the data of over 60 million students and more than 18,000 customers – namely school systems – worldwide, was infiltrated by cybercriminals who accessed highly Sensitive Information of students and educators. The cybercriminals obtained unauthorized access to certain PowerSchool Student Information System ("SIS") through its PowerSource portal.[5]

34. Upon information and belief, the cybercriminals gained access to Plaintiffs and Class Members' PII with the intent of misusing this PII, including marketing and selling Plaintiffs' and Class Members' PII.

35. Defendants did not alert customers (mainly schools and school districts) until January of 2025 – 10 days after detecting the Data Breach. Even then, Defendants still have not

[4] *PowerSchool's Privacy Principles*, POWERSCHOOL, https://www.powerschool.com/privacy/ (last accessed January 16, 2025).

[5] *Incident General FAQs*, POWERSCHOOL (January 17, 2025), https://www.powerschool.com/security/sis-incident/.

alerted all customers regarding the Data Breach, including parents, students, and faculty who have been impacted by the Data Breach.

36. In January 2025, Defendants sent a letter to affected school districts and their customers informing them that:

> As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.[6]

37. Omitted from this letter was the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

38. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

39. Subsequently, "PowerSchool confirmed that this was not a ransomware attack but it did pay a ransom to prevent the data from being released."[7]

40. Moreover, in its data breach notice disclosure letter, Defendants failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their

---

[6] https://go.powerschool.com/index.php/email/emailWebview?email=ODYxLVJNSS04NDYAAAGX4Uc94samuzXqzBdCGatRdeJwgal900VGXSgoP85TrLnvepWYYq-7EeVcjgepIFIOPZ5zgR8gxxuMKsVpqwO8EOo5zfHJaOHLA.

[7] James Coker, *PowerSchool Reportedly Pays Ransom to Prevent Student Data Leak*, INFOSECURITY MAGAZINE (Jan. 9, 2025), https://www.infosecurity-magazine.com/news/powerschool-pays-ransom-data-leak/.

data, whether Class Members should report their misuse to Defendants, and whether Defendants set up any mechanism for Class Members to report any misuse of their data.

41. Defendants had obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

42. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

43. The attacker accessed and acquired files containing unencrypted PII of Plaintiffs and Class Members. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

44. Plaintiffs further believe that Plaintiffs' PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

45. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic data security procedures.

Defendants' Failed Response to the Data Breach

46. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII with the intent of misusing the PII, including marketing and selling Plaintiffs' and Class Members' PII.

47. On January 7, 2025 – nearly two weeks after it claims to have first discovered the Data Breach – Defendants finally began communicating to school districts and its customers that certain PII was potentially compromised as a result of the Data Breach.[8] This communication provided basic details of the Data Breach and Defendants' recommended next steps.

[8] *Supra*, n.5.

48. PowerSchool has acknowledged that the information accessed in the Data Breach included at least the following for students and educators:

a. the individual's name,

b. contact information,

c. date of birth,

d. limited medical alert information,

e. Social Security Number (SSN), and

f. other related information.

49. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base.

50. Plaintiffs and Class Members were required to provide their PII to Defendants in order to receive services. Thus, Defendants created, collected, and stored Plaintiffs' and Class Members' PII with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

51. Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

52. Despite this, Plaintiffs and Class Members remain, even today, in the dark regarding what specific data was stolen, the particular malware used and what steps are being taken, if any, to secure their PII going forward.

53. Plaintiffs and Class Members are left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes.

54. Indeed, Plaintiffs and Class Members are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

55. Plaintiffs' and Class Members' PII may end up for sale on the dark web or simply fall into the hands of companies that will use the detailed PII for targeted marketing without

Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Plaintiffs' and Class Members' PII.

Defendants Collected/Stored Class Members' PII

56. Defendants acquired, collected, stored, and assured reasonable security over Plaintiffs' and Class Members' PII.

57. As a condition of its relationship with Plaintiffs and Class Members, Defendants required that Plaintiffs and Class Members entrust Defendants with highly sensitive and confidential PII. Defendants, in turn, stored that information on Defendants' system that was ultimately affected by the Data Breach.

58. By obtaining, collecting, and storing Plaintiffs and Class Members' PII, Defendants assumed legal and equitable duties over the PII and knew or should have known that it was thereafter responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

59. Plaintiffs and Class Members have taken reasonable steps to maintain their PII's confidentiality. Plaintiffs and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to only make authorized disclosures of this information.

60. Defendants could have prevented the Data Breach by properly securing and 4 encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' PII.

61. Defendants' negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

62. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendants was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants is a large, sophisticated operation with resources to put adequate data security protocols in place.

63. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs' and Class Members' PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

64. In failing to adequately secure Plaintiffs' and Class Members' sensitive data, Defendants breached duties it owed Plaintiffs and Class Members under statutory and common law.

65. Plaintiffs and Class Members surrendered their highly sensitive PII to Defendants under the implied condition that Defendants would keep it private and secure.

66. Accordingly, Defendants also had an implied duty to safeguard their PII, independent of any statute.

67. Defendants was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015).

68. In addition to its statutory obligations, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' PII.

69. Defendants owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that all PII in its possession was adequately secured and protected.

70. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

71. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

72. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

73. Defendants owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust their PII to Defendants.

74. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probably victims of any inadequate security practices.

75. Defendants owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

76. Indeed, central to its core business, PowerSchool collects highly personal data for tens of millions of students, parents, and school faculty. It generates hundreds of millions of dollars annually through the collection, storage, and use of this information. It therefore had ample resources and a strong motive to adopt reasonable protections. It also should have known that such protections were necessary given the highly personal nature and value of information it stores.

77. PowerSchool knew or should have known that it would almost certainly be the target of hackers. Similar education technology providers have been subject to data breaches in previous years. More recently, PowerSchool informed the FBI that it was subject to a campaign to obtain PowerSchool's data.

Defendants' Insufficient Data Security Caused the Data Breach

78. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information that they were maintaining for Plaintiffs and Class

Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

79. Security experts, both private and governmental, have long warned companies that data security must be a top priority. The Federal Trade Commission ("FTC"), for example, has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[9] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[10]

80. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

81. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

82. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45 ("FTC Act").

---

[9] *Start with Security A Guide for Business, Lessons Learned from FTC Cases*, FEDERAL TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] *Id.*; *Protecting Personal Information, A Guide for Business*, FEDERAL TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[11] *How to Protect Your Networks from RANSOMWARE*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view at 3 (last accessed on Jan. 24, 2025).

83. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶7 (June 15, 2011) ("[Defendants] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶7 (Mar. 7, 2006) ("[Defendants] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendants] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all proceeded Defendants' Data Breach, further clarify the measures businesses must take to meet their data security obligations.

Defendants Failed to Comply with FTC Guidelines

84. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45.[12]

[12] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. The FTC's publication, "*Start with Security: A Guide for Business*," sets forth cybersecurity guidelines and best practices for businesses.[13] These guidelines note, *inter alia*, that businesses should: (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on computer networks; (d) understand network vulnerabilities; (e) implement policies to correct security problems. The FTC guidelines further recommend that all businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[14]

86. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

87. Defendants were at all times fully aware of its obligation to protect the PII of students, faculty, and parents because of its position as a business associate, which gave it direct access to reams of student, faculty, and parent PII from school districts with which it contracts. Defendants were also aware of the significant repercussions that would result from its failure to do so.

88. Despite its obligation, Defendants failed to properly implement basic data security practices, and Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

The Data Breach was a Foreseeable Risk of which Defendants was on Notice

[13] *What To Do Right Away*, FTC, https://www.identitytheft.gov/Steps (last accessed on Jan. 24, 2025).

[14] *Id.*

89. It is well known that PII is highly sensitive and is a frequent, intentional target of cybercriminals. Companies that collect and handle such information, including Defendants, are well aware of the risk of being targeted by cybercriminals.

90. Defendants also knew that a breach of its computer systems, and exposure of the sensitive information stored therein, would result in harm to such individuals.

91. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[15]

92. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. According to the IRTC, in 2022, there were 1,802 reported data compromises in the United States, the second highest number of data events in a single year and only 60 events short of the record high number of events that occurred in 2021.[16] Of the 1,802 compromises reported in 2022, 98.4% were data breaches, affecting at least 392,180,551 victims in total, and 83% involved the exposure of sensitive records.[17]

93. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. The Bureau of Justice Statistics reported that, in 2021, about 23.9 million people in the United States were victims of an identity theft incident, and their losses totaled $16.4 billion.[18] The increasing rate of identity theft is apparent from the directly preceding Bureau of Justice publication, which covered the data from

[15] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[16] *Data Breach Reports: 2022 End of Year Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 25, 2023), https://www.idtheftcenter.org/publication/2022-data-breach-report at7.

[17] *Id.* at 6, 21.

[18] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, BUREAU OF JUST. STAT. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf.

2018. From 2018 to 2021, the number of persons affected increased by approximately one million, and monetary losses increased by $1.3 billion.[19]

94. PII has considerable value and constitutes an enticing and well-known target for cybercriminals. Hackers can easily sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[20]

Defendants Failed to Comply with Industry Standards

95. As discussed herein, experts studying cybersecurity routinely schools and school district and partners as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

96. Several best practices have been identified that at a minimum should be implemented, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

97. Other best cybersecurity practices that are standard across industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

98. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

[19] Erika Harrell, *Victims of Identity Theft, 2018*, BUREAU OF JUST. STAT. (Apr. 2021,), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

[20] Krebs, *supra*, note 15.

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

99. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Plaintiffs and Class Members Suffered Damages Due to the Data Breach

100. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

101. Cyberattacks and data breaches at companies like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

102. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

103. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[21] *See* U.S. Gov. Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

104. Moreover, theft of PII is also gravely serious. PII is an extremely valuable property right.[22]

105. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

106. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

107. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have suffered damages, including missed payments and out-of-pocket expenses associated with (i) the failure to receive payments for the services rendered to patients; (ii) costs associated with obtaining loans, lines of credit and other debts due to the failure to receive timely payment for the services rendered to patients; (iii) the costs for purchasing new healthcare payment software to process claims for payment; (iv) time spent trying to address the failure to be able to submit claims for payment, including time spent with insurance companies, time spent with patients and other third parties; and (iii) other costs resulting from the Data Breach.

Data Breaches Increase Victims' Rick of Identity Theft

108. The unencrypted PII of Class Members will end up for sale on the Dark Web as that is the modus operandi of hackers.

109. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

110. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the

[22] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.")(citations omitted).

data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

111. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

112. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages. [23]

113. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

114. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ /.

115. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

116. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

117. Then, this comprehensive dossier can be sold – and then resold in perpetuity – to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft & Fraud

118. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

119. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time – which cannot be recaptured – spent on mitigation activities.

120. Plaintiffs' mitigation efforts are consistent with the GAO Report in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

121. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),

[24] *See* U.S. Gov. Accountability Office, *supra*, n.21.

reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

122. And for those Class Members who experience actual identity theft and fraud, the GAO Report in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

Diminution of Value of PII

123. PII is a valuable property right.[27] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

124. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[28]

125. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[29]

126. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[30] [31]

---

[25] *See* Federal Trade Commission, *supra*, n.13.

[26] *See supra*, n.11.

[27] *See* U.S. Gov. Accountability Office, *supra*, n.21.

[28] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[29] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[30] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[31] *The personal data revolution*, DATACOUP, https://datacoup.com/ (last accessed on Jan. 24, 2025).

127. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[32]

128. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

129. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

130. The fraudulent activity resulting from the Data Breach may not come to light for years.

131. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

132. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

133. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, upon information and belief, tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

[32] *Nielsen Computer & Mobile Panel, Frequently Asked Questions*, NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (

134. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

135. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

136. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

137. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

138. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and a necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss of Benefit of the Bargain

139. Furthermore, Defendants' poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendants and/or its agents for educational services or agreeing to obtain employment at Defendants, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services or employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

PLAINTIFFS' EXPERIENCES

140. Plaintiff Nicholas Hisserich is the father and legal guardian of Plaintiff A.H. His daughter attends a school in the St. Charles School district in St. Charles, Missouri that uses PowerSchool products. As a result, he has provided his and his daughter's PII to PowerSchool.

141. Plaintiff A.H., a minor, brings this suit by and through her father and legal guardian, Nicholas Hisserich.

142. Plaintiff A.H. attends a school which is one of Defendants' customers.

143. As a condition of enrolling in school, Plaintiffs were required to provide their PII to Defendants.

144. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiffs PII in its system.

145. Plaintiffs are very careful about sharing their sensitive PII. Plaintiffs store any documents containing their PII in a safe and secure location. Plaintiff A.H. and her guardian have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Neither Plaintiff A.H., nor her guardian, would have entrusted their PII to Defendants had they known of Defendants' lax data security policies.

146. Plaintiff Nicholas Hisserich received the Data Breach disclosure letter, by email, directly from his daughters' school district, or about January 16, 2025. According to Data Breach disclosure letter, Plaintiff A.H's school district was one of the many school districts impacted by the Data Breach.

147. Upon information and belief, Plaintiffs' PII was improperly accessed and obtained by unauthorized third parties.

148. As a result of the Data Breach, and at the direction of the Data Breach disclosure letter, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiffs have spent significant time dealing with the Data Breach – valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

149. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

150. The Data Breach has caused Plaintiffs to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed Plaintiffs of key details about the Data Breach's occurrence.

151. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

152. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

153. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

154. Plaintiffs bring this action, individually, and on behalf of a nationwide class, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and/or 23(b)(3), defined as follows:

Nationwide Class
All individuals residing in the United States and its territories whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendants in January 2025 (the "Class").

Missouri Subclass
All residents of Missouri whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendants in January 2025 (the "Class").

155. Collectively, the Class and Missouri Subclass are referred to as the "Classes" or "Class Members."

156. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendants has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for option out, any and all federal, state, or local governments, including, but not limited to, its departments, agencies, divisions, bebeerus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

157. In the alternative, Plaintiffs may request subclasses as necessary based, *e.g.*, on the types of PII that were compromised.

158. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and the motion for class certification.

159. This action has been brought and may be properly maintained as a class action under Rule 23(b) because there is a well-defined community of interest in the litigation and membership in the proposed Classes are easily ascertainable.

160. **Numerosity**: The members of the Classes are so numerous that joinder of all members is impracticable. While the exact number and identity of individual members of the Class is unknown at this time, such information being in the sole possession of Defendants and/or third parties and obtainable by Plaintiffs only through the discovery process, Plaintiffs believes,

and on that basis alleges, that the Class consists of hundreds of thousands of people. The number of Class members can be determined based on Defendants' and other third party's records.

161. **Commonality**: Common questions of law and fact exist as to all members of each Class. These questions predominate over questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendants' wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

162. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Classes because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

163. **Adequacy**: Plaintiffs have no interest that conflicts with the interests of the Classes and are committed to pursuing this action vigorously. Plaintiffs have retained counsel competent and experienced in complex consumer class action litigation. Accordingly, Plaintiffs and their counsel will fairly and adequately protect the interests of the Classes.

164. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

165. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

166. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

167. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies and practices hinge on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiffs.

168. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

169. Finally, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

CAUSES OF ACTION

COUNT 1
Negligence
(On Behalf of Plaintiffs and the Class)

170. Plaintiffs hereby re-allege and incorporate all allegations in the Complaint, as though fully set forth herein.

171. Plaintiffs and the Class (or their third-party agents) entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

172. Defendants owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendants' failure – to use adequate data security in accordance with industry standards for data security – would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

173. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

174. Defendants owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiffs' and Class members' PII.

175. Defendants owed – to Plaintiffs and Class members – at least the following duties to:

a. Exercise reasonable care in handling and using the PII in its care and custody;

b. Implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. Promptly detect attempts and unauthorized access;

d. Notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

176. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

177. Defendants also had a duty to exercise appropriate practices to remove PII it was no longer required to retain under applicable regulations.

178. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and use of the PII belonging to Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

179. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendants with their confidential PII, a necessary party of obtaining services from Defendants.

180. The risk that unauthorized persons would attempt to gain access to PII, and misuse it, was foreseeable by Defendants. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII – whether by malware or otherwise.

181. PII is highly valuable, and Defendants knew, or should have known, that the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

182. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

183. Defendants breached these duties as evidenced by the Data Breach.

184. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII by:

a. Disclosing and providing access to this information to third parties; and

b. Failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

185. Defendants breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

186. Defendants further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries-in-fact.

187. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

188. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs, and Class members have suffered, continue to suffer, or will suffer damage, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

189. And, on information and belief, Plaintiffs' PII has already been published – or will be published imminently – by cybercriminals on the Dark Web.

190. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

191. Defendants' breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs' and Class members' actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, lost access to their banking accounts; and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which Plaintiffs and Class members continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(on Behalf of the Plaintiffs and Class)

192. Plaintiffs hereby re-allege and incorporate all allegations in the Complaint, as though fully set forth herein.

193. Under the FTC Act, 15 U.S.C. §45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

194. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs' and the Class members' sensitive PII.

195. Defendants breached their respective duties to Plaintiffs' and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security

practices to safeguard PII. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

196. The harm that has occurred is the type of harm that the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

197. But for Defendants' wrongful and negligent breach of its duties owed, Plaintiffs and Class members would not have been injured.

198. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants were failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

199. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

200. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(on behalf of Plaintiffs and the Class)

201. Plaintiffs hereby re-allege and incorporate all allegations raised in the Complaint, as though fully set forth herein.

202. Plaintiffs and Class members either directly contracted with Defendants or Plaintiffs and Class members were the third-party beneficiaries of contracts with Defendants.

203. Plaintiffs and Class members (or their third-party agents) were required to provide their PII to Defendants as a condition of receiving services provided by Defendants. Plaintiffs and Class members (or their third-party agents) provided their PII to Defendants or its third-party agents in exchange for Defendants' services.

204. Plaintiffs and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid Defendants would be used to pay for adequate cybersecurity measures.

205. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

206. Plaintiffs and the Class members (or their third-party agents) accepted Defendants' offers by disclosing their PII to Defendants or its third-party agents in exchange for services.

207. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII to unauthorized persons.

208. In its Privacy Policy, Defendants represented that they had a legal duty to protect Plaintiffs' and Class Members' PII.

209. Implicit in the parties' agreement was that Defendants would provide Plaintiffs and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII.

210. After all, Plaintiffs and Class members (or their third-party agents) would not have entrusted their PII to Defendants (or their third-party agents) in the absence of such an agreement with Defendants.

211. Plaintiffs and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendants.

212. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties

according to their terms, means preserving the spirit – and not merely the letter – of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

213. Defendants materially breached the contracts it entered with Plaintiffs and Class members (or their third-party agents) by:

a. failing to safeguard their PII;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information;

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendants created, received, maintained, and transmitted.

214. In these and other ways, Defendants violated their duty of good faith and fair dealing.

215. Defendants' material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

216. And, on information and belief, Plaintiffs' PII has already been published – or will be published imminently – by cybercriminals on the Dark Web.

217. Plaintiffs and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(on Behalf of Plaintiffs and the Class)

218. Plaintiffs hereby re-allege and incorporate all allegations in the Complaint, as though fully set forth herein.

219. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

220. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiffs' and Class members' PII is highly offensive to a reasonable person.

221. The intrusion was into a place or thing which was private and entitled to be private.

222. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendants, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

223. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

224. Defendants acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

225. Defendants acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

226. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

227. As a proximate result of Defendants' acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

228. And, on information and belief, Plaintiffs' PII has already been published – or will be published imminently – by cybercriminals on the Dark Web.

229. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendants with their inadequate cybersecurity system and policies.

230. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PII of Plaintiffs and the Class.

231. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(on Behalf of Plaintiffs and the Class)

232. Plaintiffs hereby re-allege and incorporate all allegations in the Complaint, as though fully set forth herein.

233. This claim is pleaded in the alternative to the breach of implied contract claim.

234. Plaintiffs and Class members (or their third-party agents) conferred a benefit upon Defendants. After all, Defendants benefitted from using their PII (and/or payment) to provide services.

235. Defendants appreciated or had knowledge of the benefits it received from Plaintiffs and Class members (or their third-party agents).

236. Plaintiffs and Class members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

237. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII.

238. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

239. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and Class members' PII and/or payment because Defendants failed to adequately protect their PII.

240. Plaintiffs and Class members have no adequate remedy at law.

241. Defendants should be compelled to disgorge into a common fund – for the benefit of Plaintiffs and Class members – all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(on Behalf of Plaintiffs and the Class)

242. Plaintiffs hereby re-allege and incorporate all allegations in the Complaint, as though fully set forth herein.

243. Given the relationship between Defendants and Plaintiffs and Class members, where Defendants became guardian of Plaintiffs' and Class members' PII, Defendants became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

244. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendants' relationship with them – especially to secure their PII.

245. Because of the highly sensitive nature of the PII, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendants, or anyone in Defendants' position, to retain their PII had they known the reality of Defendants' inadequate data security practices.

246. Defendants breached their fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII.

247. Defendants also breached their fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

248. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Declaratory Judgment
28 U.S.C. §2201
(on Behalf of Plaintiffs and the Class)

249. Plaintiffs hereby re-allege and incorporate all allegations raised in the Complaint, as though fully set forth herein.

250. Under the Declaratory Judgment Act, 28 U.S.C. §2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, that are tortious and that violate the terms of the federal and state statutes described in this Complaint.

251. Plaintiffs seek a declaration of the rights of the parties under the Federal Declaratory Judgement Act, 28 U.S.C. §2201.

252. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendants' actions were – and still are – inadequate and unreasonable.

253. Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

254. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed – and continues to owe – a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants have a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continue to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants breach of its duties caused – and continues to cause – injuries to Plaintiffs and Class members.

255. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

256. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experience a second data breach.

257. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages – while warranted for out-of-pocket damages and other legally quantifiable and provable damages – cannot cover the full extent of Plaintiffs' and Class members' injuries.

258. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

259. An injunction would benefit the public by preventing another data breach – thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request that this Court:

A. Determine that the claims alleged herein may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and issue an order certifying one or more of the Classes defined above;

B. Appoint Plaintiffs as the representative of the Class and their counsel as Class counsel;

C. Award declaratory and other equitable relief as necessary to protect the interests of the Plaintiffs and Class;

D. Award injunctive relief as necessary to protect the interests of the Plaintiffs and the Class;

E. Enjoining Defendants from further unfair and/or deceptive practices;

F. Award Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

G. Award restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

H. Award reasonable attorneys' fees and costs;

I. Award prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

K. Grant such further relief that this Court deems appropriate.

JURY DEMAND

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Dated: February 3, 2025

LEXINGTON LAW GROUP, LLP

s/ Patrick Carey

Patrick Carey (CA Bar No. 308623)
503 Divisadero St.
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
pcarey@lexlawgroup.com

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Joseph P. Guglielmo*
Ethan S. Binder*
Anja Rusi*
The Helmsley Building
230 Park Ave., 24th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
ebinder@scott-scott.com
arusi@scott-scott.com

Attorneys for Plaintiffs and the Putative Class

Pro hac vice forthcoming